жатся уже готовые статистические данные и инструментарий, позволяющий, зная данные об уязвимостях и их вероятностях, определить возможные и актуальные угрозы, в том числе с учетом перечня угроз, указанных в [6].

Библиографические ссылки

1. *Кирсанов С. В.* Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли //Докл. ТУСУР. 2013. № 2 (28). С. 115–118.

2. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие для вузов. М. : Горячая линия-Телеком, 2004. 280 с.

3. *Семкин С. Н., Беляков Э. В., Гребенев С. В., Козачок В. И.* Основы организационного обеспечения информационной безопасности объектов информатизации : учеб. пособие. М. : Гелиос АРВ, 2005. 192 с.

4. *Домарев В. В.* Безопасность информационных технологий. Системный подход. К. : ООО «ТИД ДС», 2004. 992 с.

5. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры : утв. зам. директора ФСТЭК России 18 мая 2007 г.

6. *Вихорев С. В.* Классификация угроз информационной безопасности. М. : ОАО «ЭЛВИС-ПЛЮС», 2001.

МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ФАЙЛОВЫХ СИСТЕМАХ

Д. В. Куц
(Екатеринбург, УрФУ, Qcmail@rambler.ru)

Защита информации в файловых системах чрезвычайно важная и актуальная тема в области информационной безопасности.

Сбой файловой системы часто приносит не меньше проблем, чем отказ физического носителя. Восстановление информации оказывается делом трудным, длительным, а часто и невыполнимым. Очень многое в этом процессе зависит от используемой файловой системы. Поэтому вопросы надежности, защиты целостности фай-

лов, отказоустойчивости, возможности восстановления зачастую имеют решающее значение при выборе файловой системы. Для большинства файловых систем полное восстановление данных на сильно фрагментированном томе после форматирования, ошибочного удаления или серьезного сбоя – задача практически невыполнимая.

Разграничение доступа в файловых системах также является актуальной темой, имеющей большой потенциал в развитии, поскольку возможностей наиболее распространенной дискреционной модели во многих случаях оказывается недостаточно. В некоторых случаях целесообразна поддержка мандатной, ролевой, тематической модели разграничения доступа средствами файловой системы.

Криптографическая защита данных файловой системы должна обеспечивать не только безопасность, но и доступность данных для легального пользователя. Необходимо искать разумный компромисс между стойкостью защиты и удобством ее использования. Например, выход из строя микросхемы TPM на материнской плате или самой платы (что случается нередко) во многих случаях делает расшифровку данных на томе, зашифрованного с помощью BitLocker, весьма проблематичным. Стойкость шифрования EFS напрямую зависит от стойкости пароля пользователя, зашифровавшего данные или имеющего разрешение на доступ к ним, а также агента восстановления, если таковой имеется в системе.

Еще одной актуальной проблемой является адаптация файловой системы к типу используемого носителя для обеспечения его большей отказоустойчивости и более длительного жизненного цикла. Для жестких дисков важными являются вопросы обеспечения максимально возможного быстродействия файловой системы. В первую очередь, за счет минимизации перемещений считывающих головок при работе с файлами. В этом случае носитель будет функционировать и надежно хранить данные более длительное время при прочих равных условиях. В случае же использования твердотельных накопителей SSD или Флэш-карт на первое место встает вопрос минимизации количества циклов записи в одни и те же ячейки памяти. На данный момент уже разработано несколько файловых систем, оптимизированных для работы с флэш-памятью, однако

бурный рост производительности и скоростей работы данной памяти будет требовать корректировки алгоритмов работы файловых систем в сторону повышения надежности и отказоустойчивости, возможно, за счет снижения быстродействия.

ПРОБЛЕМЫ ДЕЦЕНТРАЛИЗАЦИИ ХРАНЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО РАСПРОСТРАНЕНИЯ НА ПРЕДПРИЯТИИ

В. С. Лужнов
(Челябинск, ЮУрГУ, ua9stz@gmail.com)

На сегодняшний день практически каждое предприятие, независимо от масштабов и форм осуществляемой деятельности, активно использует системы информатизации и автоматизации. В особенной степени это касается применения компьютерных систем для обработки и хранения информации. Активный рост рынка систем электронного документооборота [1] и государственные инициативы, направленные на адаптацию законодательства под современные тенденции [2], подтверждают, что потребность в переходе от бумажного к электронному хранению документации на предприятиях становится все острее.

При этом наиболее частым решением в качестве технической реализации выступает централизованное хранение всей информации предприятия на специально выделенном компьютерном комплексе (сервере). Очевидно, что при такой организации все процессы, связанные с хранением и обработкой информации, становятся зависимыми от качества работы комплекса. Его полный или частичный выход из строя может нанести значительный ущерб всему предприятию в целом.

Другой фактор, связанный с информатизацией процессов функционирования, выражается в экспоненциальном росте объемов генерируемой предприятием информации. Потребность в долгосрочном хранении больших объемов электронных данных и необходи-